U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

The Management of the National Nuclear Security Administration's Classified Enterprise Secure Network Project

DOE/IG-0823 September 2009

Department of Energy
Washington, DC 20585

September 16, 2009

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on the "Management of the National Nuclear Security Administration's Classified Enterprise Secure Network Project"

BACKGROUND

In June 2000, recently enacted legislation directed the National Nuclear Security Administration (NNSA) to "perform planning, analysis, testing and evaluation necessary to develop the highest value alternatives for improving cyber security throughout the Nuclear Weapons Complex." In response, NNSA began the Integrated Cyber Security Initiative. Through the initiative, NNSA's Enterprise Secure Network (ESN) was developed. ESN was intended to be the primary network for sharing classified information within NNSA by: ensuring the protection of nuclear weapon and other national security information; supporting the NNSA mission; and, replacing NNSA's existing classified network, SecureNet.

Over time, the Office of Inspector General has identified many concerns regarding the design of Department management information system networks, including numerous cases where Department projects have been completed behind schedule and/or have exceeded their established budgets. For example, a 2001 audit of the Department's *Telecommunications Infrastructure* (DOE/IG-0537) highlighted the existence of duplicative data transmission infrastructures across the Departmental complex. Because of the importance of effectively managing information technology projects and controlling classified electronic information, we initiated this audit to determine whether the NNSA ESN project was adequately managed and was meeting its intended goals and objectives.

RESULTS OF AUDIT

We found that neither the planning for nor execution of the ESN project had been effective. Furthermore, this process had led to a system which did not meet certain pre-established goals and objectives:

- Despite nine years of development and the expenditure of at least $153 million, ESN only recently became fully operational. This was three years after its planned completion date. While capable of transmitting classified data,

approximately 150 software applications used for classified processing had not been certified or approved for operation on the network; and,

- Although initially justified and planned as the network provider for all of NNSA's Advanced Simulation and Computing (ASC) supercomputers and other classified systems, the network lacked sufficient capacity for such traffic. This necessitated the continued operation and maintenance of separate classified networks.

These issues were attributable, in large part, to problems with planning and management of the ESN effort. For example, in spite of Department requirements to the contrary, ESN planning and development did not incorporate project management controls and protections required for efforts anticipated to cost more than $20 million. As a result, NNSA had not properly tracked project costs for the first seven years of the development effort. In our judgment, the lack of visibility over costs most likely contributed to a recent announcement by NNSA that the project had been completed for $60 million when, in fact, it would have been more accurate to acknowledge that over twice this amount, more than $153 million, had been expended on the effort since inception.

Because of the lack of project management rigor, senior NNSA management officials were deprived of the information necessary to ensure that the ESN initiative was properly planned and executed, apply generally recognized best practices, and to properly track project costs. In addition, because of delays in ESN becoming operational, certain other NNSA initiatives dependent upon it, including ongoing efforts to standardize and consolidate weapons data and enforce need-to-know access across the NNSA complex, had been adversely impacted. Without general improvements in project management, future NNSA information technology projects, including these designed to enhance and upgrade ESN, may continue to experience delays and higher than necessary costs.

Beginning in 2006, NNSA made an effort to improve project oversight by developing limited ESN documentation and instituting cost tracking. While helpful, these actions did not ensure that ESN and similar projects were adequately managed throughout their lifecycle, providing good taxpayer value. Ensuring that projects are based on sound project management principles and that they closely adhere to cost and schedule controls are attributes that will be critical as the Department continues its implementation of the *American Recovery and Reinvestment Act of 2009*. In these challenging economic and budget times, taxpayers should expect that projects such as ESN and other significant efforts are well managed and provide good value. Accordingly, we have made recommendations, which if fully implemented, should help increase the return on investment of ESN and future NNSA information technology related projects.

MANAGEMENT REACTION

NNSA management concurred with our recommendations and stated that they believed several actions taken recently will improve the program's project management capabilities. However, they did not agree with the report's conclusions in a number of areas. While we consider management's recent actions to be positive steps, we feel that

more improvement is needed to ensure that ESN and other major information technology projects are adequately managed throughout their lifecycle. Management's comments, which are significant, are more fully discussed in the body of this report and are included in Appendix 3.

Attachment

cc: Deputy Secretary
Chief of Staff
Administrator, National Nuclear Security Administration
Chief Information Officer
Chief Information Officer, NNSA

REPORT ON THE MANAGEMENT OF THE NATIONAL NUCLEAR SECURITY ADMINISTRATION'S CLASSIFIED ENTERPRISE SECURE NETWORK PROJECT

TABLE OF CONTENTS

The Management of the National Nuclear Security Administration's Classified Enterprise Secure Network Project

Enterprise Secure Network Project Management

The National Nuclear Security Administration's (NNSA) Classified Enterprise Secure Network (ESN) project had not been effectively planned and executed and was not meeting certain goals and objectives. Specifically, we identified issues in the timeliness of project implementation, accounting for project costs, and in meeting all planned project goals and objectives.

Project Functionality and Costs

After nine years of development and expenditures totaling about $153 million, ESN only recently became fully operational – over three years after its estimated completion date. An internal project tracking system established during the early stages of the project determined that all aspects of the network, including full operation at each of the NNSA sites minus certain limited functionality, were to be completed by 2006. However, none of ESN's sites were operational in 2006. Furthermore, at the time we completed our audit work, no sites were using ESN for its intended purpose, to transmit classified data between sites. Specifically, all site network connections had not been completed and only limited production data was being transmitted over ESN. Only recently, after the completion of our field work, was ESN made fully operational. While now capable of transmitting classified data, the compatibility of the estimated 150 applications that would be running on ESN had still not been completely reviewed to ensure their use on the network would not create security issues.

Even though specifically required by Department of Energy (Department) project management directives for projects of this cost and magnitude, NNSA Headquarters did not track all costs associated with ESN. NNSA officials were unable to provide an accurate accounting of costs for the ESN project. Although we identified an internal project tracking system developed in 2003 that estimated it would cost $116 million to complete the project, officials acknowledged that historically, ESN expenditures were not captured separately, but instead were tracked as part of overall cyber security spending. A specific reporting code for the tracking of ESN funds was not designated by NNSA until fiscal year (FY) 2006 – seven years into the project.

Nonetheless, an NNSA official recently reported an on-budget completion of the ESN project, with expenditures of approximately $60 million. We were unable to determine, and management could not supply information to support how the reported cost of $60 million was calculated. In contrast, based on varying information provided by NNSA, we calculated that costs for the project incurred by the end of our review ranged between $153 million and $180 million. Specifically, based on summaries of project funding received between FY 2000 and FY 2008, we calculated $153 million – approximately 155 percent more than reported and 32 percent over budget – had been spent to develop the network. Furthermore, officials associated with the project at its inception stated that, beginning in 2000, $20 million per year was set aside for the development of the network – totaling $180 million. We noted that an additional $33 million had been requested for FY 2009, a portion of which was for continued development and enhancement of the network.

Network Goals and Objectives

Although ESN was initially funded and approved on the basis that the network would contain specified capabilities, such as the ability to handle all NNSA classified network traffic, including classified data from the Advanced Simulation and Computing (ASC) supercomputers, project managers subsequently made the decision to scale back the project's scope. This decision resulted in ESN being constructed without the necessary capacity to handle all NNSA classified data. Such action required the continued use of a separate network infrastructure for the ASC supercomputer traffic.

The ESN Program Management Plan, originally developed in 2004 and updated in 2007, acknowledged that maintaining separate secure infrastructures weakens security by adding unnecessary complexity; thus leading to different, costly, and potentially incompatible solutions. Specifically, the Program Management Plan stated that NNSA's Integrated Cyber Security Initiative "*… coordinates with core NNSA initiatives, campaigns, and programs, including ASC and ADAPT, to ensure that the secure infrastructure and environments needed by the NNSA activities are available. Without the ESN, each activity would be responsible for providing its own secure infrastructure thus leading to different, costly, and likely incompatible solutions. Separate secure infrastructures would*

also substantially weaken security by adding unnecessary complexity to the networks and inhibiting the secure sharing of information among the NNSA programs." In spite of this acknowledgment and understanding, decisions to limit capacity of ESN will require that NNSA and the Department program offices continue to maintain multiple infrastructures to transmit classified data.

Management Attention and Oversight

NNSA did not meet its initial objectives for the ESN project or implement the network in the most effective manner because management did not focus sufficient attention on implementing project management requirements and generally accepted best practices for projects of this magnitude. Also, it did not have in place strong management oversight over project costs and development.

Project Management

NNSA management had not adhered to established project management requirements and generally accepted best practices to effectively manage the ESN project over its lifecycle. To ensure goals are met, the Department requires all projects with costs expected to exceed $20 million to pass five specific milestones, known as Critical Decisions, in the areas of Mission Need, Alternative Selection, Performance Baseline, Construction, and Start of Operation. To gain approval at each Critical Milestone to proceed to the next phase, specific documentation requirements must be met. However, certain project documentation essential for effective management had not been developed, consistently maintained and/or approved for ESN. Although the project was initiated in late 2000, much of the documentation was developed after 2006, by which time the project had already received over $100 million and was to have originally been completed. Specifically, we identified 36 studies, decision points, or evaluations required by Department project management regulations and applicable to the ESN project, 26 of which had not been completed and 9 that were completed in 2006 or later. For example:

- An acquisition strategy had not been developed to describe the high-level business and technical management approach designed to achieve project objectives within specified resource constraints. The acquisition strategy must be approved by the Program Secretarial Officer and conveys the project team's approach for the successful acquisition of the project,

its intended outcomes, and the rationale for that approach. Additionally, it is a critical project management tool since it serves as the framework for planning, organizing, staffing, controlling and leading a project;

- Project performance baselines had not been formally established, validated, and adjusted as needed for key parameters such as schedule, cost and scope. Although early project management tools contained a project timeline and cost estimate, these were not revisited and adjusted for changes after 2005. Performance baselines are critical to enable management to effectively track the project and determine whether it is being delivered on time and within estimated costs;

- A Project Execution Plan had not been developed to establish the initial policy and procedures to be followed to manage and control the project, including information regarding the organization of and schedule for the project. One key element included in the Project Execution Plan is the critical path which determines the tasks that must be completed or partially completed before other tasks begin and assists in ensuring that the project is executed in a timely manner; and,

- An Earned Value Management System (EVMS) had not been utilized by the project team. The Department requires that all projects having a Total Project Cost greater than or equal to $50 million use an EVMS. An EVMS integrates the technical, schedule and cost aspects of a project and provides integrated performance measurement for monitoring and controlling the project.

Also, documentation provided by NNSA contained conflicting information, such as varying site lists for connectivity and inconsistent connectivity schedules. Specifically, we noted that documentation detailing sites scheduled for connection to ESN ranged from 9 to 12 sites.

Additionally, the ESN project lacked the executive level management attention necessary to increase the likelihood of success. Successful performance of Department projects depends on professional and effective project management by the Federal Project Director. The appointment of the Federal

Project Director is one of the activities in Critical Decision 1, *Approve Alternative Selection & Cost Range*. This individual must champion the project and ensure it meets cost, schedule and performance targets. The project director must also establish and charter an Integrated Project Team. We noted that such a team had not been chartered for the ESN project.

DOE Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, requires project directors to be certified to ensure that projects are managed with integrity and in compliance with applicable laws. However, since the project's inception, NNSA has assigned responsibility for ESN to at least three different individuals, none of whom were officially appointed to manage the project. Further, only one of these individuals was a certified project manager. When questioned regarding training levels, NNSA officials stated that the current project manager was in the process of obtaining the necessary certification.

Project Tracking

Despite estimated project costs of more than $153 million, cost information was not effectively tracked and reported throughout the project's lifecycle. Specifically, Office of Management and Budget (OMB) Exhibit 300s were not consistently developed and submitted for the ESN project over the past nine years. We noted that Exhibit 300s were submitted until 2005, but were then discontinued until just recently when a submission was made in 2008. Exhibit 300s are required of all investments in excess of $5 million and are designed to coordinate OMB's collection of agency information for its reports to Congress required by the *Clinger-Cohen Act of 1996*. Additionally, the Exhibit 300 helps ensure that the business case for an investment is made and tied to mission statements, long-term goals and objectives, and annual performance plans developed pursuant to the *Government Performance and Results Act of 1993* (GPRA). ESN was also not consistently captured in the agency's OMB Exhibit 53, which provides summary information for all information technology (IT) investments in an agency's investment portfolio. Information in the Exhibit 53 allows OMB to review and evaluate each agency's IT spending for comparison across the Federal Government.

Similarly, the ESN project was not tracked in the Department's Project Assessment and Reporting System (PARS) from its

inception. The Department requires that all projects costing $5 million or more be tracked in PARS. This system is designed to provide Department executive management with the information necessary to properly oversee ongoing projects. NNSA officials did not input ESN information into PARS until October 2006, seven years into the project; however, this was the only submission made. We also noted that although an internal tracking system had been developed for distributing time and deliverables over the life of the ESN project, it had not been updated or maintained since September 2005, despite continued delays in implementation and changes in project scope.

Opportunities for Improvement

As a result of ineffective application of project management requirements and best practices, executive management was unable to maintain visibility over and properly manage the ESN project. In particular, management officials lacked up-to-date information on project tracking data necessary to determine if the project was being delivered on time and within budget. NNSA officials also could not determine, based on information available to them, if funds were being properly spent and if resources needed to be reallocated. Based on a comparison of project cost estimates and our analysis of costs, we calculated that the ESN project had a cost overrun of at least $37 million and was delivered three years beyond its planned completion date. The ESN project should have been completed in 2006 at an overall cost of around $116 million. However, as noted above, the network only recently became fully operational, and using conservative estimates, we calculated that project costs totaled over $153 million.

Without improvements in project management, future NNSA IT projects, to include enhancements and upgrades to ESN, may continue to experience delays and higher than necessary costs. For example, due to the lack of an acquisition strategy, ESN network components were procured earlier than necessary. As a result, project officials stated that some hardware had become obsolete or reached the end of its lifecycle and must be replaced prior to ESN being fully operational at all sites. In addition, officials stated that numerous enhancements will be added to ESN over the course of the next few years. Officials added that they plan to consider these future enhancements, such as the "Need-to-Know" software application, as separate projects. This practice may cause these project segments to fall under the Department's project management and reporting thresholds.

Supplemental guidance to OMB Circular A-11 allows agencies to compartmentalize projects into smaller, more workable sections; however, all segments must still be managed and reported as one overall project.

Because of delays in completing ESN, program managers have been unable to completely review the compatibility of approximately 150 applications for use on ESN. These applications are necessary for NNSA classified program operations. In light of significant network changes brought about by ESN and the absence of these reviews, NNSA officials cannot ensure their use on the network does not create security issues for NNSA's classified programs.

RECOMMENDATIONS

To help ensure the effective management of NNSA's Classified ESN project and to ensure that project management requirements and best practices are followed for all ongoing and future IT projects, we recommend that the Administrator, NNSA:

1. Adhere to existing Department requirements for management, to include:

   - Development of a detailed project plan, which contains timelines for key deliverables and assignment of responsible individuals, for completion of all remaining ESN development and implementation tasks; and,

   - Accurate accounting for all project costs.

2. Complete and submit the documentation required by OMB, as well as the Department, to include Exhibits 300 and 53; and,

3. Coordinate with other program offices within the Department and the Office of the Chief Information Officer (OCIO), to determine the most efficient and effective way to meet the Department's classified networking needs.

MANAGEMENT AND AUDITOR COMMENTS

While NNSA management concurred with the recommendations, they disagreed with certain conclusions reached in the report. Management commented that corrective actions had been initiated prior to the issuance of the draft

version of the report. As a result, they stated that they believed the intent of the recommendations had been met, and therefore should be considered closed.

Although management's comments regarding actions taken are noteworthy, they are not fully responsive to our recommendations. In addition, as noted, we feel that the recommendations should be forward looking and applied to all ongoing and future IT projects. Therefore, we believe this precludes the recommendations from being considered complete and closed. However, we have modified the wording of the recommendations to ensure that our intent to include all IT projects is better recognized. Management's comments on our recommendations are summarized below, followed by our response.

Report Recommendations

In response to Recommendation 1, management included details regarding the corrective actions taken as an attachment to their comments. The attachment listed 17 items that had been put in place in the past year. These included the establishment of a governance process; implementation of an Earned Value Management (EVM) component; and the development of several other components designed to complement the operation of the network. For each of the actions listed, additional consideration of approach or detail is needed, certain activities are in formative stages, and completion periods have either not been reached or were not provided. For example, management did not state whether the EVM tool they have procured was certified by the American National Standards Institute (ANSI), as required by Department directive. We noted that the process to receive ANSI certification is lengthy. Also, we believe that 14 of the 19 items were integral to the successful development and operation of the network and should have been implemented much earlier, not during the final year of a nine-year development effort.

With regard to Recommendation 2, management noted that the ESN FY 2004 Exhibits 300 and 53 had been updated to reflect the current status of the ESN project and cost associated with the project. Management's actions in this regard are noteworthy. Our recommendation in this area is meant to be forward looking to help ensure that required OMB and Department documentation, such as this, is completed and

submitted consistently for all ongoing and future projects, as necessary.

Management's comments were not responsive to Recommendation 3. Therefore, planned actions for coordinating still need to be addressed with other Department programs performing NNSA mission-related work and the Department's OCIO to determine the most effective way to meet the overall classified networking needs. With such actions, NNSA and the Department as a whole would be able to take advantage of future opportunities for operational savings, such as the connection of non-NNSA sites to ESN for performing NNSA-related mission work.

Management also provided specific comments on the report. Management's comments are summarized below, followed by our auditor response. Management's comments are included in Appendix 3.

Project Development

Management commented that the report focuses solely on ESN development over the past nine years, but does not include other major components that were a part of the Integrated Cyber Security Initiative (ICSI). In addition, management contended that the report incorrectly noted nine years of development and expenditures of at least $153 million for the ESN project when, in fact, ESN took four years to complete with actual cost to develop and deploy of approximately $70 million. Management explained that the difference between these amounts was actually spent on developing the other components of ISCI.

We agree that NNSA initiated the ICSI Program in response to Congressional direction to improve its cyber security posture and that the initiatives included all of the segments listed. However, we believe that all of these activities were undertaken in support of ESN; and, therefore, should have been considered part of the overall project. Specifically, the FY 2005 budget justification submitted to Congress stated that: *"The Integrated Cyber Security Initiative (ICSI) provides the definition, planning, and design efforts for the development and deployment of the NNSA enterprise-wide secure network (ESN)."* We also noted that the budget justification outlined ten elements of ICSI, nine of which focused on ESN. As indicated, the ICSI Program was initiated in 2000 in direct

support of ESN. Thus we concluded that planning and development of ESN actually began in late 2000 and ended in FY 2009 when the network became operational – nine years later. Furthermore, actual expenditures for development of ESN as stated in the most recent Exhibit 300 (budget year 2010) – which management emphasized noted in its comments had been updated and now reflected the current state of the ESN project – totaled $153.14 million.

Network Goals and Objectives

Management stated that as with its predecessor, SecureNet, ESN supports only the control information needed to run the bulk transfers between the supercomputers that are part of the Advanced Simulation and Computing (ASC) Initiative. As such, management stated that ESN was not intended to provide the necessary bandwidth for the total ASC bulk transfer requirements. As noted in the body of the report, the Program Management Plan stated that the original intent of ESN was to consolidate and replace numerous classified connections throughout NNSA, including ASC. However, the initial plan to consolidate all classified networks was subsequently changed.

Networked Applications

Management stated that the ESN Security Plan "grandfathered" all of the existing applications and protocols in use at the time the SecureNet Security Plan was retired (March 2009). This was done to allow continued support for programmatic needs during the infrastructure transition from SecureNet to ESN. Management pointed out that certification and accreditation (C&A) is the responsibility of the site hosting the application, thus meeting its requirements. Management asserted that reporting that "approximately 150 software applications" had not been certified or approved for operation on the network was factually inaccurate. We partially agree with NNSA's position and have modified the report to better reflect our position that the security review of applications should have been performed prior to introducing them into the operating environment.

Management Attention

Management commented that the NNSA Management Council received a quarterly progress and performance briefing from

the ESN Project Manager. However, we believe that without complete and accurate cost information, these briefings could not have been fully beneficial to NNSA. In addition, an essential element of IT project oversight is the Department's IT Capital Planning and Investment Control (CPIC) Process. The CPIC Process is intended to provide senior level visibility for the Department's and NNSA's major IT investments to ensure that they remain within cost and schedule baselines. The audit team noted that, until recently, ESN was not part of this process and when it began being tracked by the Department's IT Council (in the 1st quarter FY 2009), it was given a score of "Red" because no data was submitted.

Management also stated that the NNSA OCIO had two independent reviews conducted, one in March 2006 that concurred with the approach taken by the project lead to implement ESN and a second review in March 2008 that determined the project requirements had been completed. However, in informal comments to our draft report, management stated that as a result of the March 2006 review, the CIO directed the project be restructured. Our review of the March 2006 assessment disclosed that the review team felt that the project was viable, but suggested several changes including the establishment of a Project Management Office. As such, we believe that management's assertion that the March 2006 assessment concurred with the approach taken by the Project Lead to implement ESN is inconsistent with the results of that assessment.

Exit Conference Comments

During the exit conference to discuss management's comments, NNSA officials provided additional observations regarding the draft report. Officials believed that ESN had been effectively managed by two project managers, but acknowledged that project documentation and support had not always been maintained or kept current. For example, officials stated that although ESN had been re-baselined to exclude the ASC supercomputers due to security concerns, project documentation had not been revised to reflect this change. Furthermore, NNSA officials indicated that a business decision was made to permit about 150 software applications to operate on ESN based on the accreditation that was granted for SecureNet, the predecessor to ESN. They added that actions were still ongoing to ensure that these applications fully satisfy security requirements for operating on ESN. In addition, a

Memorandum of Understanding was subsequently provided relating to this decision. The officials also indicated that significant progress had been made to satisfy the recommendations contained in the report. One NNSA official stated that the Office of Inspector General (OIG) was correct in its assessment of the management of the ESN project, including our determination that the project had been delivered over budget and behind schedule. However, this official added that despite initial problems, ESN largely achieved its expected results.

The OIG supports NNSA management in its efforts to satisfy report recommendations and thereby improve IT project management, both on the ESN project and future efforts. In reference to the certification documentation pertaining to the aforementioned 150 software applications, we noted that the SecureNet documentation was not dated and contained an expiration date of March 31, 2009. Therefore, that certification did not adequately support prior and current approval for operating these applications on ESN. Furthermore, in light of the significant network changes brought about by ESN, consistent with Federal and Department requirements, these 150 applications should have either been certified prior to operation on ESN or addressed in the certification letter signed by the Designated Approving Authority supporting acceptance of the risk on an interim basis and tracked in a plan of actions and milestones until the risk was mitigated.

Appendix 1

OBJECTIVE

To determine if the National Nuclear Security Administration's (NNSA) Classified Enterprise Secure Network (ESN) project is meeting its intended goals and objectives and is being adequately managed.

SCOPE

The audit was performed between May 2008 and May 2009 at Department of Energy (Department) Headquarters in Washington, DC, and NNSA Headquarters in Washington, DC.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable laws and directives pertaining to project management;
- Reviewed applicable standards and guidance issued by Office of Management and Budget;
- Analyzed NNSA-provided documentation pertaining to the development and cost of ESN;
- Held discussions with officials from the Department and NNSA; and,
- Reviewed reports by the Office of Inspector General and the Government Accountability Office.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and NNSA's implementation of the *Government Performance and Results Act of 1993* and determined that it had not established performance measures for information technology project management. Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely on computer-processed data to satisfy our objectives. An exit conference was held with Department officials on September 9, 2009.

Appendix 2

RELATED REPORTS

- Special Report "*Management Challenges at the Department of Energy*" (DOE/IG-0782, December 2007). Based on work performed over the past year, the report identified both cyber security and project management as two of the most serious challenges facing the Department of Energy (Department). Over the past few years, the area of "information technology (IT)," which encompassed a broad range of IT contracts, programs, and security, had been classified as a management challenge. Recently, threats to the Government's information systems have risen to become a national security risk. As a result of these risks and in light of recent efforts to intrude into the Department's systems, we have categorized Cyber Security as a significant management challenge. In addition, for several years, the Office of Inspector General, the Government Accountability Office, and the Department itself have designated project management as a high-risk area vulnerable to waste, fraud, and abuse. In numerous cases, Department projects have been completed behind schedule and exceeded established budgets. In recent years, the Department, in responding to identified weaknesses in the area of Project Management, has sought to improve the discipline and structure of project performance. However, due to a variety of reasons, our reviews continue to highlight concerns in the area of Project Management.

- *The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007). The audit found that the Department had not fully achieved the goals and objectives envisioned by the original Department of Energy Common Operating Environment initiative. These problems occurred because officials responsible for implementation did not always follow Department and Federal project management practices, such as developing formal migration plans and conducting requirements analyses. In addition, procedures relating to user account termination were not adequate. As a consequence, the Department was unable to complete the Headquarters conversion within established timeframes and is unlikely to realize originally anticipated cost savings.

- *The National Nuclear Security Administration's Implementation of the Federal Information Security Management Act* (DOE/IG-0758, February 2007). The audit identified a number of deficiencies that exposed critical unclassified systems to an increased risk of compromise. These weaknesses included incomplete or inadequate system certification and accreditation; weak continuity of operations planning; and, unresolved system control deficiencies. We found that NNSA did not always properly implement its own guidance as well as Departmental and Federal cyber security requirements. In addition, NNSA had not performed regular monitoring activities essential to evaluating the adequacy of cyber security program performance. As a consequence, NNSA's unclassified information systems and networks and the data they contain remain at risk of being compromised, including the possible unlawful diversion of operational data, personally identifiable information, or other critical information.

- *Telecommunications Infrastructure* (DOE/IG-0537, December 2001). The audit disclosed that duplicative data transmission infrastructures existed across the Departmental complex. These problems occurred because the Department had not

developed and implemented a coordinated approach to the acquisition and use of telecommunications equipment and services. Further, the Department had not adopted a comprehensive set of performance measures and incentives which would have encouraged both Federal employees and contractors to obtain necessary telecommunication capabilities as cost effectively as possible. As a consequence, the Department annually spends at least $4 million more than necessary to operate and maintain its telecommunications infrastructure.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

June 18, 2009

MEMORANDUM FOR: Rickey R. Hass
Deputy Inspector General
for Audit Services

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to IG Draft Report on NNSA's Enterprise Secure Network; Proj. No. A08TG056; IDRMS No. 2008-01386

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report entitled *The Management of the National Nuclear Security Administration's Classified Enterprise Secure Network Project.* We understand that the purpose of this audit was to determine if the Enterprise Secure Network (ESN) was within cost, scope, milestones, intended objectives, and being adequately managed.

Based on the information contained in the report, NNSA believes that the report contains numerous incorrect conclusions about the ESN project. NNSA does agree with the recommendations, and in fact, we have already implemented them, as described in the attachment of detailed actions that NNSA has taken over the past year to improve the Project Management capabilities of the ESN project.

In June 2000, Congress directed NNSA to develop processes and procedures for improving cyber security throughout the Nuclear Weapons Complex. In response to this direction, NNSA began the Integrated Cyber Security Initiative (ICSI). The ICSI Program consisted of many components, including ESN, Information Assurance Response Center (IARC), classified infrastructure enhancements (i.e., the Los Alamos National Laboratory [LANL] Red Network), Continuous Asset Monitoring System (CAMS), Integrated Certification and Accreditation System (ICAS), and logical access improvements (i.e., Homeland Security Presidential Directive [HSPD] 12).

The IG's report focuses solely on ESN development and implementation over the past nine years, but does not include other major projects within the ICSI Program. However, the report incorrectly notes nine years of development for the ESN project, and expenditures of at least $153M. In fact, ESN took *four* years to complete, and the actual cost to develop and deploy ESN was approximately $70M. The $83M difference

between these amounts, as identified in the report, was actually spent on developing the IARC, classified infrastructure enhancements (LANL Red Network), CAMS, ICAS, and logical access improvements (HSPD-12).

The report further states that ESN was intended to replace SecureNet as the interface between all classified networks, and to replace Distance Computing and Distributed Computing (DISCOM) for supercomputing activities. The SecureNet Security Plan referenced by the report was an "umbrella" security plan that covered limited classified connections between sites. DISCOM was developed by the Application for Site Certificate (ASC) Project. The purpose for DISCOM was to provide bulk transfer connectivity for supercomputers between laboratories that SecureNet could *not* provide in its single connection design. As with its predecessor SecureNet, ESN supports only the control information needed to run the bulk transfers that DISCOM provides. Similarly, the ESN connection is a single physical connection up to 1-Gb/s and never was intended to have the necessary bandwidth for the total ASC connectivity requirements of up to 4-Gb/s. However, the SecureNet Security Plan not only contained the single SecureNet connection, but also provided a security plan for the DISCOM connections. In assuming the SecureNet Security Plan, ESN "owns" the SecureNet and DISCOM connections (TACLANES) from a security standpoint. The physical DISCOM connections and the TACLANES are part of the ESN Security Plan and listed in the Interconnect Security Agreements (ISAs) for Lawrence Livermore National Laboratory (LLNL), LANL, and Sandia National Laboratories (SNL). This was accomplished so that the SecureNet Security Plan and the old security plans (referred to as SecureNet Access Subnet plans) at each site could be retired, which was accomplished in March 2009. All networks are functioning as they were designed with ESN replacing SecureNet.

As related to the applications referenced in the report, the ESN Security Plan grandfathered all of the old existing applications and protocols in use at the time the SecureNet Security Plan was retired (March 2009). This was done to allow continued support for NNSA programmatic needs during the security infrastructure transition from SecureNet to ESN. As with SecureNet, ESN was not designed to accredit or certify applications--certification and accreditation (C&A) is the responsibility of the site hosting the application, thus meeting their requirements.

ESN accredits and certifies its own core applications, but does not certify or approve site applications. The report states that "approximately 150 software applications" had not *been certified or approved for operation on the network. This is factually inaccurate.* These applications were grandfathered-in and are covered by a security plan usually a site plan while transmission between sites is covered by the ESN Security Plan. An ESN Transition Plan is currently in process; the grandfathered-in applications will have a security review and be strengthened accordingly, to ensure that all applications are up to ESN standards.

The report also stated that NNSA senior leadership was not aware of the information needed to ensure properly planned and executed best practices for project management. The NNSA Management Council received a quarterly progress and performance briefing

from the ESN Project Manager. Results of the briefings included personnel changes driven by the NNSA Office of the Chief Information Officer (OCIO). The Chief Information Officer (CIO) replaced the Project Leader for ESN (in November 2007). The replacement was made to ensure that increased technical knowledge and oversight was in place to senior leadership on project planning and management activities. A dedicated Program Project Lead was hired by the CIO (in January 2008), to ensure proper management of the ESN Project. The OCIO also had two independent reviews conducted, one in March 2006 and one in March 2008. The results of the March 2006 review concurred with the approach taken by the Project Lead to implement ESN. The March 2008 review determined that the project requirements had been completed.

Regarding the recommendations contained in the report to improve overall project management of the ESN project, including establishing a full-time ESN Project Manager, developing a detailed project plan, and completing Exhibits 300 and 53 for ESN. Under the direction of the CIO, a full-time ESN Project Manager was added to the OCIO staff in January 2008. The ESN 2004 Exhibit 300 and 53 have been updated to reflect the current status of the ESN project and cost associated with the project. All of the recommendations were initiated prior to the issuance of this draft IG report. NNSA believes that the intent of the recommendations has been met, and considers them closed.

If you have any questions regarding this response, please contact Cathy Tullis, Acting Director, Policy and Internal Controls Management, 586-3857.

Attachment

cc: Linda Wilbanks, Chief Information Officer
Karen Boardman, Director, Service Center
David Boyd, Senior Procurement Executive

Attachment: Detail Actions to the Recommendations

Under the leadership of the Office of the Chief Information Officer (OCIO) the ESN leadership has put in place a number of initiatives and processes in the past year to improve the Project Management capabilities of the ESN project. We have made rapid progress by hiring several new highly qualified PM practioners and by focusing our efforts on implementing Project Management best practices in accordance with the Project Management Institute (PMI) and the Project Management Book of Knowledge (PMBOK). Following is a short discussion of some of our new ESN processes and accomplishments that have been made during the past year:

1. **Built an Application Integration (AI) Component.** The AI Team has developed a comprehensive User's Guide outlining the procedures they follow in order to integrate an application onto ESN. It provides a standardized set of procedures all AI Team members follow in working with site representatives or application owners. Additionally, they are working on an Application Survey designed to gather technical information and application requirements during the requirements phase of the integration project. Currently, the Team has completed integration of 7 applications and has 14 in progress.

2. **Built a Configuration Management (CM) Component.** The CM Team has designed and built a complete CM process and program based on industry best practices and relevant work already completed at Pantex. The Team has published a CM Plan and Release Management Plan and integrated both into the CM process. Additionally, we have purchased an automated CM tool and designed an interface with our NIARC trouble ticket process.

3. **Built a Risk Management (RM) Component.** Using a value-driven methodology which links ESN risks to NNSA strategic goals and objectives, the RM program has been integrated into normal project operations. Additionally, the RM Team has written an ESN Risk Management Plan and a comprehensive Risk Management Matrix which captures and mitigates all technical and operational risks.

4. **Built a Metrics Component.** Based on the principles of the Risk Management Program, the RM Team continued the paradigm into a metrics program that captured and measured our progress on three levels; Strategic, Operational and Tactical. The Team completed the initiative by designing a qualitative approach to not only measure progress, but also to graphically represent progress to executive level OCIO management.

5. **Built an Integrated Master Schedule (IMS) to include Resource Loading.** The Work Brake-down Schedule (WBS) for our new IMS has been restructured to better facilitate costing and the implementation of Earned Value reporting. Additionally, procedures have been established to update/status the IMS every two weeks.

6. **Implemented Earned Value Management (EVM) Component.** Based on industry best practices, we have implementing a rigorous EVM process designed to capture and report progress status. We have purchased a commercial EVM tool to support this effort.

7. **Built Operators Training Component.** Based on NNSA security and site requirements, we designed a comprehensive 3-day Operators Training Course which meets our annual training requirements. Our Training Lead selected subject matter experts from throughout the community to present training on appropriate technical and operational issues. This course has been given in a professional environment at the Nevada Site Office twice this past year and to 30 students each time. We conduct an after-action session to determine changes that need to be made to follow-on courses. To date, we have built the Operator-level training but are also working on other relevant courses.

8. **Built Subject Matter Expert (SME) Component.** Completing a thorough analysis of our SME pool, it was determined we were "thin" in certain very technical areas of expertise. To mitigate the risk of an SME shortage, we developed a program to identify candidate SME personnel, provide the right level of training, assign the candidate to a mentor with work projects, complete an evaluation, then add the person to our official list of SME personnel. This way, we have a back-up in all technical areas and always have a person in the training cycle to enhance our SME population.

9. **Built Logistics Management Component.** Realizing the critical need to keep our network hardware and software current and secure, while constantly striving to protect our shrinking budget, we consolidated all logistics and acquisition initiatives under the Director of Operations and a member of the A-Team staff. When a requirement is identified, approved and funded, it enters our supply chain management system and the action is tracked from item procurement to delivery and is always under a single logistics manager for accountability. The Director of Operations approves all hardware moves throughout the program and the Logistics Manager is accountable for all equipment inventories.

10. ***Designing Operation Standards Component for 2010.*** As ESN is developed, deployed and enhanced, the need to ensure operational procedures and standards are maintained becomes increasingly important. Thus, based on after-action reviews from training sessions, analysis of network trouble tickets, weekly Operations and A-Team telephonic meetings, we are designing an Operational Standards Program which will be executed in 2010. This initiative will be formulated in a standardized document and the Operations Team will visit each ESN site to review operator's knowledge of established procedures. A result of this program will be updated procedural documents and training courses.

11. **Instituted Quarterly OCIO Status Briefing Component.** Designed to keep the OCIO briefed on current status of a complicated project, we designed a Quarterly OCIO Status Briefing. This briefing was presented 3QFY09 and is scheduled again in the 4th quarter. Covering all critical functional areas, the briefing starts with a current risk analysis then progresses through engineering, operations, budget, critical path, metrics and pressing personnel issues.

12. **Built Enterprise Architecture (EA) Component.** Although still in the design phase, the PM has designated a Lead Enterprise Architect from the A-Team and tasked him to design an EA program consistent with DOE regulations and guidelines. The Lead Architect is currently writing an EA Plan and actively working with PRIDE initiatives. Our architecture must be developed to support future technology enhancements plus and the plethora of other applications scheduled to be integrated into ESN.

13. **Building an Enterprise Data Resource Management (EDRM) Component.** Based on the findings of the EA initiative, the PM has recently established an EDRM Team and tasked an A-Team member to lead it. The EDRM Team is chartered to ensure the development and execution or architectures, policies, practices and procedures properly manage the full data lifecycle needs of the ESN enterprise.

14. **Built Transition Plan.** The Director of Operations is managing the development of a plan and organized process designed to monitor all site secure networks, report on the traffic being passed, analyze its content, and determine any security risks that might be discovered. This initiative is responsible to ensure all possible risks are identified and mitigated to the satisfaction of the Cyber Security Program Manager and Enterprise DAA. Personnel supporting this team consist of the Network Operations Center (NOC) lead, A-Team members, and security analysts for the Security Engineering Board (SEB).

15. **Built New Site Integration Team.** The Operations Team has developed a team of experts in the field of new site integrations. We learned from the initial ESN site integration, that this is a complimented process. Therefore, we designated a team to be the advanced party to do the site coordination, site survey, *requirements gathering, and configuration determination. Based on apparent new* site needs, we designed and tested 3 different equipment configurations which can be emplaced in new sites. Additionally, the Site Integration Team provides information of network costs, personnel skill sets and training required. This Team has developed a detailed New Site Checklist which is provided to any site that anticipates a connectivity requirement.

16. **Established Governance Process.** Based on the *Governance Performance and Results Act of 1993*, our newly formed Project Management Office (PMO) has made significant progress towards establishing the appropriate internal controls in

accordance with NNSA's implementation guidance. Our PMO instituted performance measurement and metrics, developed a detailed project plan and schedule, re-established the documentation required for OMB Exhibits 300 and 53.

17. **Coordinating with Product Realization Integrated Digital Enterprise (PRIDE) Community.** The PM realized that we needed to be extremely close to the PRIDE community of users and develop in parallel to their customer needs. Therefore, we embedded 2 A-Team members in their activities and have constant coordination with their initiatives. Our AI Team members built their application priority list in concert with PRIDE requirements.

18. **PM Qualifications.** The ESN PM is making significant progress towards achieving DOE level III PM status.

19. **Weekly Staff Meetings.** Established weekly Project Management Office (PMO) staff meetings and added a professional development element to our staff training requirements.

IG Report No. DOE/IG-0823

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.energy.gov

Your comments would be appreciated and can be provided on the Customer Response Form.